DOI: 10.23977/acss.2021.050102
ISSN 2371-8838

Secure Lossy Transmission over Wiretap Channels with Side Information and State Information

Muyu Hu[1, *], Ming Xu[1, 2]

[1]*College of Information Engineering, Shanghai Maritime University, Shanghai 201306, China*

[2]*College of Electronicsand Information Engineering, Tongji University, Shanghai 201804, China*

*Corresponding author

Keywords: secure lossy transmission, wiretap channel, side information, state information, information leakage.

Abstract: This paper investigates the problem of secure lossy transmission over wiretap channels with side information and state information. Aiming at the reliability and security of compressed pictures, videos and other files when they are transmitted, a wiretap channel model with side information and state information and a secure lossy source transmission scheme based on double binning technique under this model are proposed. By using Fano inequality and Csiszár sum identity, the inner bounds of transmission rate, distortion rate and information leakage rate are proved. Considering noisy situations in reality, the Gaussian noise channel under this model is analyzed concretely as an example. Based on error estimation and differential entropy theorem, the inner bounds of transmission rate and distortion rate are obtained. Moreover, the equivocation rate is introduced to transform the information leakage rate into the minimum mean square error of the estimated source and its outer bound is also obtained. The simulation results show that under the optimal conditions of the proposed system model, the transmission rate can reach 0.7315 bits/source bit, the distortion rate can reach 0.0052 bits/source bit and the information leakage rate can reach 0.1286 bits/source bit.

1. Introduction

With the development of network information technology, the amount of information generated in various fields has shown explosive growth. Among them, sensitive and private information, such as feature data in biometrics [1], electronic images of health examination recorded in medical system [2], video files in company Cloud Services [3], data sources in streaming media applications [4] and ecommerce transaction data set [5]. Transmission processing is particularly important. There is a huge amount of raw information that has not been processed. To transmit efficiently, compression is needed. How to ensure the security of transmission is a problem. Information theory improves the security of the system by studying the basic limits of information flow in network transmission and the optimal coding scheme to reach these limits.

Secure transmission of information sources based on information theory was first proposed by Shannon [6]. On this foundation, Wyner proposed wiretap channel and it was assumed that the wiretap channel was degraded compared with the legal channel, the message can be transmitted safely in noise channels [7]. Csiszár and Körner extended this conclusion to general broadcast channels. According to the uncertainty of the eavesdropper to the transmitted information, they measured the security level of the channel. They also established a rate-leakage region for public and confidential messages [8]. Slepian and Wolf did some research on the source coding with side information and get the corresponding achievable transmission rate region [9]. The above work is based on the secure and lossless transmission of the source. That is to say, the legal receiver reconstructs the source without distortion when the source is compressed and transmitted. If the source produces distortion during compression and transmission, we should consider the influence of distortion on the security during transmission. Wyner and Ziv defined the rate-distortion function $R(D)$ in source secure lossy transmission. They also added limited constraints such as rate, distortion and leakage rate. Its purpose is to keep the eavesdropper as unknown as possible to the transmitted message [10]. Chia and Chong described the rate-distortion region of Wyner-Ziv source coding with side information. It was pointed out that feedback from decoder to encoder would not reduce the total rate [11]. Villard and Piantanida studied the secure multi source coding problem when the side information is noncausal to the decoder. In addition, the inner and outer bounds of the rate-distortion-equivocation region are derived [12]. On the basis of these, they built the channel model that side information was noncausal to eavesdroppers. When the non-coding side information is noncausal to the legitimate users and the source received by legitimate users can be reconstructed without damage, a tighter rate-distortion-equivocation region is obtained [13]. Furthermore, Xu et al. used the degraded side information to refine the Gaussian vector source coding problem and they also used MSE(Mean Square Error) to derive rate-distortion region[14]. Considering that the statistical characteristics of wireless fading channels are constantly changing, Koyluoglu et al. introduced state information and indexed broadcast channels which had states. Finally, the OCP(Optimal Corner Points) and the distance between the outer bound and the achievable region are obtained[15]. Han et al. proposed a wiretap channel model in which the state information is available noncausally at the encoder and derived the inner bound of secrecy capacity and the key capacity of degraded wiretap channel [16].

Through the above analysis, it can be seen that the side information can help the decoder to reduce the distortion rate between the source and the source estimation and the state information can be used to characterize the wireless fading channel with uncertain statistical characteristics and improve the message transmission rate. However, due to the complexity of the wireless channel, especially in the wireless fading wiretap channel, it often contains both side information and state information. How to design a secure and reliable encoding and decoding mechanism and delimit the related limited bit rate constraints needs further research. This paper proposes a secure lossy transmission scheme in which the side information is available noncausally at the decoder and the state information is also available noncausally at the encoder. According to the statistical difference among the side information, state information and channel noise, the inner bound of rate-distortion-information leakage rate is obtained and the optimal trade-off among the three is obtained. The reliability and security of the model are judged by what we obtained.We considering a secure lossy transmission model with side information and state information in wiretap channel, in which the side information is available noncausally at the decoder and the state information is also available noncausally at the encoder. The coding scheme is designed based on the system model and double binning technique. The inner bound of rate-distortion-information leakage rate is determined by combining joint typicality lemma, Fano Inequality, Csiszár Sum Identity and other information theories. The proof of achievability and the proof of converse are given. Taking the Gaussian noise wiretap channel under the system model as an example, the inner bounds of rate and distortion rate are derived. Then the information leakage rate is transformed into the minimum mean square error of the estimated source by introducing the equivocation rate. Finally, the outer bound of the minimum mean square error of the source estimation is obtained and the proof is given. Considering the difference of noise power between the legitimate channel and wiretap channel, the difference of side information noise power between legitimate receiver and eavesdropper and the difference of state information noise power between the legitimate receiver and eavesdropper, we have simulated the inner bounds of rate, distortion and information leakage rate under various conditions. Finally, the optimal trade-off among the three is obtained and the experimental results are compared and analyzed.

2. System model

2.1 Notation

The entropy function $H(\cdot)$ denotes the uncertainty about the random variable. Mutual information $I(\cdot)$ denotes the information about a random variable obtained from the observation of another random variable; X, Y and Z denote the discrete random variables on the finite set $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$. x, y and z denote the values of X, Y and Z. Let X, Y and Z be three random variables on some alphabets with probability distribution $P(x)$, $P(y)$ and $P(z)$, respectively. If $P(x|yz)=P(x|y)$, then they form a Markov chain, which is denoted by $X-Y-Z$. Notation x_k^n stands for the collection $(x_k, x_{k+1}, ..., x_n)$ for any sequence $(x_i)_{i\in \mathrm{N}^*}$, in which N^* represents the set of positive natural numbers. x_1^n is simply denoted by x^n. Random variable Y is said to be less noisy than Z w.r.t. Y if $I(\mathrm{U;Y}) \geq I(U;Z)$ for each random variable U such that $U-X-(Y,Z)$ form a Markov chain. Let P, Q be two jointly scalar Gaussian random variables with the covariance matrix Γ_{PQ}. Conditional variance of Gaussian variables is calculated by $\Gamma_{P|Q}$. $\mathbb{R}$ denotes the real line and $\mathbb{R}^d$ denotes the \$d\$-dimensional real Euclidean space.

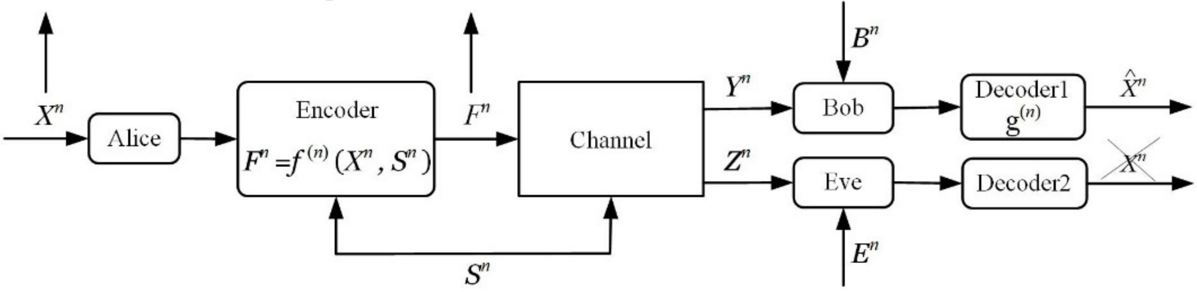


Figure. 1 Secure transmission of source over wiretap channels with side information and state information

The system model over the noise wiretap channel with side information and state information is illustrated in Fig.1, which includes the transmitter Alice, the receiver Bob and the eavesdropper Eve. Alice wants to convey information to Bob in a way that Bob can reconstruct the source within a certain distortion, and meanwhile Eve is kept ignorant of the source as much as possible. Alice, Bob, and Eve observe the sequences of random variables $(X_i)_{i\in \mathrm{N}^*}$, $(B_i)_{i\in \mathrm{N}^*}$ and $(E_i)_{i\in \mathrm{N}^*}$ respectively, which take values on $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{Z}$, respectively. X^n denotes the source. Y^n denotes the side information received by Bob. E^n denotes state information received by Eve. Side information B^n is available noncausally at the decoder. State information S^n is available noncausally at the encoder. They are independent of channel noises. Alice input source $X \in \mathcal{X}$. $Y \in \mathcal{Y}$ and $Z \in \mathcal{Z}$ output at Bob and Eve, respectively . Assuming that an expected average transmission power constraint P such that $\sum_{\mathrm{i}=1}^{n} E(x_i^2(j,S^n)) \le nP, j \in [1,2^{nR}]$, where the expectation is over the random state sequence S^n. Assume that $\bar{F}$, $\bar{U}$ and $\bar{V}$ are the sequences received by Bob and $\tilde{F}$, $\tilde{U}$ and $\tilde{V}$ are the sequences received by Eve. An (n,R) code for secure lossy source coding is defined by the encoding function $f^{(n)}$ at the transmitter: $X^n \times S^n \to F^n$, the decoding function $g^{(n)}$ at the legitimate user: $Y^n \times B^n \to X^n$.

Definition 1. Let $\hat{\mathcal{X}}$ be a reconstruction alphabet and define a distortion measure as the mapping $d{:}\mathcal{X} \times \hat{\mathcal{X}} \to [0,\infty)$. This mapping measures the cost of representing the symbol x by the symbol $\hat{x}$. The average distortion between x^n and $\hat{x}^n$ is defined as

$$d(X^n,\hat{X}^n) = \frac{1}{n}\sum_{i=1}^{n} d(x_i,\hat{x}_i) \tag{1}$$

Definition 2. If the random variable X is uniformly distributed on the set $\mathcal{X}$, the information leakage rate corresponding to $(2^{nR},n)$ secret code is defined as

$$I_e = \frac{1}{n} I(X^n;Z^n,E^n) \tag{2}$$

Definition 3. A tuple $(R,D,I_e) \in \mathbb{R}_+^3$ is said to be achievable if, for any $\delta > 0$, $n \ge 1$, there exists an $(n,R+\delta)$ code such that:

$$\mathrm{E}[d^n(X^n,\hat{X}^n)] \le D+\delta \tag{3}$$

$$\frac{1}{n} I(X^n;Z^n,E^n) \le I_e + \delta \tag{4}$$

Theorem 1. A tuple $(R,D,I_e) \in \mathbb{R}_+^3$ is said to be achievable if

$$R \ge I(V;F\,|\,B), \tag{5}$$

$$D \ge \mathrm{E}[d(X,\hat{X}(\bar{V},B,Y))], \tag{6}$$

$$I_e \ge I(X;\tilde{V},\tilde{F},B) - I(X;B\,|\,\tilde{U},\tilde{F}) + I(X;E\,|\,\tilde{U},\tilde{F}), \tag{7}$$

for some U , V satisfying the Markov chain $U - V - (X,F) - (B,E)$ and $U - V - (F,S) - (Y,Z)$. U and V denote the auxiliary random variables on the finite set $\mathcal{U}$, $\mathcal{V}$. Function $\hat{X}(V,B,Y)$ stands for source decoding sequence function.

Proof. **1) Proof of achievability**. Achievability is proved by a random coding scheme based on the double binning technique. The scheme details are given in section III.

Analysis of the rate. Define the transmission rate of the source as $R+\delta$, $\delta \to 0$, where δ represents the error value in the transmission.

There exists $R+\delta > I(U;F) - I(U;B) + I(V;F\,|\,U) - I(V;B\,|\,U) \overset{(a)}{=} I(V;F) - I(V;B) \overset{(a)}{=} I(V;F) - I(V;B)$, where (a) follows from the Markov chain $U - V - (X,F) - (B)$, and (b) follows from the Markov chain $V - F - B$.

Analysis of the distortion. Record 'Fault' as errors in the encoding or decoding step. $E(d(X^n,g^{(n)}(Y^n,B^n))] \le P\{\overline{\text{Fault}}\}E[d(X^n,g^{(n)}(r_u,Y^n,B^n))\,|\,\overline{\text{Fault}}] + P\{\text{Fault}\}E(d_{\max})$

$\le \frac{1}{n}\sum_{i=1}^{n} E[d(X_i, \hat{X}_i(C_2(r_v), Y, B)) \mid \overline{Fault}] + \varepsilon = E[d(X, \hat{X}(\bar{V}, Y, B))] + \varepsilon \le D + \varepsilon$, where $\varepsilon \to 0$ as $n \to \infty$.

Analysis of the information leakage rate.

$$I(X^n; Z^n, E^n) = I(X^n; \tilde{w}_f, \tilde{w}_u, \tilde{w}_v, E^n \mid C_n) \le I(X^n; \tilde{w}_f, \tilde{U}^n, \tilde{w}_v, E^n \mid C_n)$$

$$= H(X^n \mid C_n) - H(X^n, \tilde{w}_f, \tilde{U}^n, \tilde{w}_v, E^n \mid C_n) + H(\tilde{w}_f, \tilde{U}^n, \tilde{w}_v \mid C_n) + H(E^n \mid \tilde{w}_f, \tilde{U}^n, \tilde{w}_v, C_n)$$

$$= -H(E^n \mid X^n, C_n) - H(\tilde{w}_f, \tilde{U}^n, \tilde{w}_v \mid X^n, E^n, C_n) + H(\tilde{w}_f, \tilde{U}^n, \tilde{w}_v \mid C_n) + H(E^n \mid \tilde{w}_f, \tilde{U}^n, \tilde{w}_v, C_n)$$

$$\overset{(a)}{\le} - H(E^n \mid X^n, \mathrm{F}_n) + H(\tilde{w}_f, \tilde{U}^n, \tilde{w}_v \mid C_n) + H(E^n \mid w_f, \tilde{U}^n, \tilde{w}_v, C_n)$$

$$\overset{(b)}{\le} - H(E^n \mid X^n, \mathrm{F}_n) + H(\tilde{w}_f \mid C_n) + H(\tilde{U}^n \mid C_n) + H(\tilde{w}_v \mid C_n) + H(E^n \mid \tilde{w}_f, \tilde{U}^n, \tilde{w}_v, C_n)$$

$$\overset{(c)}{\le} n[-H(E \mid X, \tilde{\mathrm{F}}) + I(X; \tilde{F}) + I(\tilde{U}; X \mid \tilde{F}) + 5\delta + I(\tilde{V}; X \mid \tilde{U}, \tilde{F}) - I(\tilde{V}; B \mid \tilde{U}, \tilde{F})]$$

$\overset{(d)}{=} n[I(X; \tilde{V}, \tilde{F}, B) - I(X; B \mid \tilde{U}, \tilde{F}) + I(X; E \mid \tilde{U}, \tilde{F}) + \delta^{'}] \le n[R_i + \delta^{'}]$, where (a) follows from the facts that conditioning reduces entropy and that $C_n - (X^n, F^n) - E^n$ forms the Markov chain, (b) follows from the given codebook in Section III, F^n and U^n are functions of $\tilde{w}_f$, (c) follows from the codebook generation in Section III, the memoryless properties of the source and the side information channel, the Lemma 1 below with which we bound the term $H(E^n \mid X^n, \tilde{F}^n)$ and Lemma 2 below with which we bound the term $H(E^n \mid F^n, U^n, C^n)$, and (d) follows from the Markov chain $(B, E) - (X, F) - V - U$. Lemma 1 [17] and Lemma 2 [17] are as followed:

Lemma 1. Tuple (X^n, A^n) is jointly typical with high probability. A sequence of independent and identically distributed (i.i.d.) random variables with $Z^n \sim P(Z \mid XA)$. There exists

$$H(Z^n \mid X^n, A^n) \ge n(H(Z \mid X, A) - \delta_\theta), \tag{8}$$

Where $\delta_\theta \to 0$ as $n \to \infty$ and $\theta \to 0$ as $n \to \infty$.

Lemma 2. Tuple (A^n, U^n, Z^n) is jointly typical with high probability. C^n denotes a random codebook. There exists

$$H(Z^n \mid A^n, U^n, C^n) \le n(H(Z \mid A, U) + \delta_\theta), \tag{9}$$

Where $\delta_\theta \to 0$ as $n \to \infty$ and $\theta \to 0$ as $n \to \infty$.This completes the proof of achievability.

Proof of converse.

Analysis **of the rate.** $n(R + \varepsilon) \ge H(Y^n) \overset{(a)}{=} I(Y^n; F^n B^n) \overset{(b)}{=} I(Y^n; F^n \mid B^n)$

$$\overset{(c)}{=} \sum_{i=1}^{n} I(Y^n; F_i \mid F^{i-1} B^n) = \sum_{i=1}^{n} [I(Y^n F^{i-1} B^{i-1} B_{i+1}^n; F_i \mid B_i) - I(F^{i-1} B^{i-1} B_{i+1}^n; F_i \mid B_i)]$$

$\overset{(d)}{=} \sum_{i=1}^{n} I(Y^n F^{i-1} B^{i-1} B_{i+1}^n; F_i \mid B_i) \overset{(e)}{\ge} \sum_{i=1}^{n} I(V_i; F_i \mid B_i)$,where (a) take no account of distortion and noise, the information Bob receives is $F^n B^n$, (b) follows from the nonnegativity of mutual information, (c) follows from the chain rule of the conditional mutual information, (d) follows from the independence of the random variables F and B , and (e) follows from the nonnegativity of mutual information and $V_i = (F^{i-1}, B^{i-1}, B_{i+1}^n, Y^n), i \in \{1, \ldots, n\}$.

Analysis of the distortion. Bob uses the decoding function $g^n(\overline{w}_v, B^n)$. The decoding of each bit can be written as $g_i(\overline{w}_v, B^{i-1}, B_{i+1}^n) \triangleq \hat{X}_i(\overline{V}_i, \overline{B}_i)$ .Then we have $E[d(X^n, g^n(\overline{w}_v, B^n, Y^n))]$ $=\frac{1}{n}\sum_{i=1}^n E[d(X_i, \hat{X}_i(\overline{V}_i, \overline{B}_i, Y_i))]$. Define an independent random variable K , which uniformly distributed on the set $\{1,...,n\}$. Assume that $U=(K,U_k)$, $V=(K,V_k)$, $X=(K,X_k)$, $F=(K,F_k)$, $B=(K,B_k)$, $Y=(K,Y_k)$ and follow the Markov chain $U-V-(X,F)-B$ and $U-V-(F,S)-Y$. Finally, we have

$$\sum_{i=1}^n E[d(X_i, \hat{X}_i(\overline{V}_i, B_i, Y_i))] = \sum_{i=1}^n E[d(X_k, \hat{X}_k(\overline{V}_i, B_i, Y_i)) \mid i=k] = \sum_{k=1}^n E[d(X_k, \hat{X}_k(\overline{V}_i, B_i, Y_i))] + \varepsilon$$

$$= \sum_{k=1}^n E[d(X_k, \hat{X}_k(\overline{V}_i, B_i, Y_i))] + \varepsilon = E[d(X, \hat{X}(\overline{V}_i, B_i, Y_i))] + \varepsilon \le D + \varepsilon' \quad .$$

Therefore, $E[d(X, \hat{X}(\overline{V}_i, B_i, Y_i))] \le D$.

Analysis of the information leakage rate.

$$n(R_i+\delta) \ge I(X^n; Z^n, E^n) \ge I(X^n; Z^n, E^n)$$

$$\overset{(a)}{=} I(X^n; Z^n, \tilde{F}^n) + I(X^n; E^n \mid Z^n, \tilde{F}^n)$$

$$= H(X^n) - H(X^n \mid Z^n, \tilde{F}^n, B^n) - I(X^n; B^n \mid Z^n, \tilde{F}^n) + I(X^n; E^n \mid Z^n, \tilde{F}^n)$$

$$\overset{(b)}{\ge} \sum_{i=1}^n \{H(X_i) - H(X_i \mid Z^n, \tilde{F}^n, B^n, X^{i-1}) - [H(B_i \mid Z^n, \tilde{F}^n, B_{i+1}^n) - H(B_i \mid X_i, \tilde{F}_i)]$$

$$+ H(E_i \mid Z^n, \tilde{F}^n, E^{i-1}) - H(E_i \mid X_i, \tilde{F}_i)\}$$

$$\overset{(c)}{\ge} \sum_{i=1}^n [H(X_i) - H(X_i \mid Z^n, \tilde{F}^n, B^n, X^{i-1}, E^{i-1}) - I(X_i; B_i \mid \tilde{F}^n) + H(B_i \mid \tilde{F}_i) + I(X_i; E_i \mid \tilde{F}) - H(E_i \mid \tilde{F}_i)$$

$$- H(B_i \mid Z^n, \tilde{F}^n, B_{i+1}^n) + H(E_i \mid Z^n, \tilde{F}^n, E^{i-1})]$$

$$\overset{(d)}{=} \sum_{i=1}^n [\underbrace{I(X_i; \tilde{V}_i, \tilde{F}_i, B_i) - I(X_i; B_i \mid \tilde{F}^n) + I(X_i; E_i \mid \tilde{F}_i)}_{\overset{\det}{=} P_i} + I(Z^n, B_{i+1}^n, \tilde{F}^{n\setminus i}; B_i \mid \tilde{F}_i) - I(Z^n, E^{i-1}, \tilde{F}^{n\setminus i}; E_i \mid \tilde{F}_i)] \ ,$$

where (a) follows from the definite action at the encoder, (b) follows from Fano's inequality [18,Chapter 2.1] and the Markov chain $(F^n, S^n, X^{n\setminus i}, B_{i+1}^n, E^{i-1}) - (F_i, X_i) - (B_i, E_i)$, (c) follows from the Markov chain $(X_i, S^n, F_i^n, B_i^n) - (F^{i-1}, X^{i-1}) - (E^{i-1}, B^{i-1})$, and (d) follows from the definition of V_i and the definite action at the encoder.

By making the use of the Csiszár sum identity [18, Chapter 2.3], we have $\sum_{i=1}^n I(B_i; E^{i-1} \mid F^n, Z^n, B_{i+1}^n) - I(E_i; B_{i+1}^n \mid F^n, Z^n, E^{i-1}) = 0$. Then

$$n(R_i+\delta) \ge \sum_{i=1}^n [P_i + I(Z^n, B_{i+1}^n, E^{i-1}, \tilde{F}^{n\setminus i}; B_i \mid \tilde{F}_i) - I(Z^n, B_{i+1}^n, E^{i-1}, \tilde{F}^{n\setminus i}; E_i \mid \tilde{F}_i)]$$

$$\overset{(a)}{=} \sum_{i=1}^n [I(X_i; \tilde{F}_i, \tilde{V}_i, B_i) - I(X_i; B_i \mid \tilde{F}_i) + I(X_i; E_i \mid \tilde{F}_i) + I(\tilde{U}_i; B_i \mid \tilde{F}_i) - I(\tilde{U}_i; E_i \mid \tilde{F}_i)]$$

$\overset{(b)}{=} \sum_{i=1}^n [I(X_i; \tilde{F}_i, \tilde{V}_i, B_i) - I(X_i; B_i \mid \tilde{U}_i, \tilde{F}_i) + I(X_i; E_i \mid \tilde{U}_i, \tilde{F}_i)]$, where (a) follows from the definition of P_i and U_i , and (b) follows from the Markov chain $U_i - V_i - (X_i, F_i) - (B_i, E_i)$. This completes the proof of converse.

3. Random coding Scheme based on Double Binning Technique

According to the system model proposed in the previous section, the random coding scheme based on Double Binning Technique is designed. In the following we provide details of the random coding scheme based on Double Binning Technique.

Definition 4. Let x^n be a sequence may take values from finite sets $\mathcal{X}$, the empirical probability distribution function of x^n can be expressed as $\pi(x\,|\,x^n)=\frac{|\{i:x_i=x\}|}{n}$, $x\in\mathcal{X}$. Then by the law of large numbers, $\pi(x|x^n)\to P(x)$ in probability. For $X\sim P(x)$ and $\varepsilon\in(0,1)$, define the set n-sequences $\varepsilon-$typical [18] as

$$T_\varepsilon^n(X)\triangleq\{x^n:|\pi(x\,|\,x^n)-P(x)|\le\varepsilon P(x)\},x\in\mathcal{X}\,. \tag{10}$$

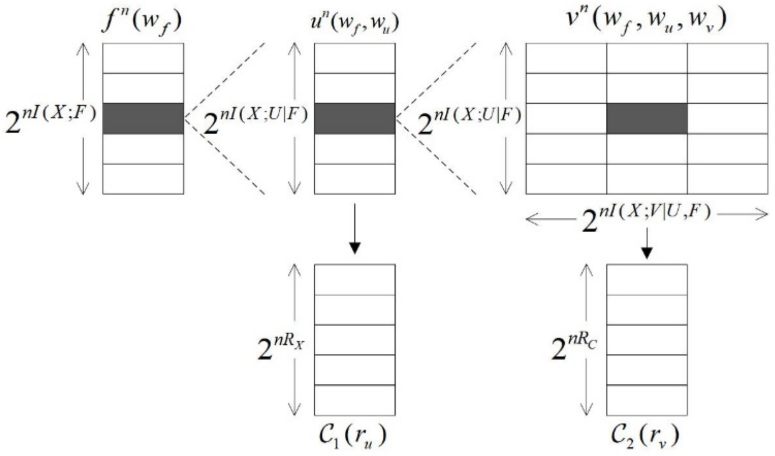


Figure. 2 Scheme Codebook.

Codebook generation. The codebook generation process is shown in Fig.2. Fixing $P_{F|X}P_{V|XF}P_{U|V}$ makes it reach the channel capacity. Randomly and independently pick $2^{nI(X;F)}$ sequences $f^n(w_f),w_f\in\{1,...,2^{nF}\}$ according to $p(f^n)=\prod_{i=1}^{n}P_F(f_i(w_f))$.

For each w_f , randomly and independently generate $2^{nI(U;X|F)}$ sequences according to $p(u^n)=\prod_{i=1}^{n}P_{U|F}(u_i\,|\,f_i(w_f))$. Then distribute $u^n(w_f,w_u)$ uniformly at random into 2^{nR_X} bin $\mathcal{C}_1(r_u)$, $r_u\in\{1,2,...,2^{nR_X}\}$. Each bin consists of $2^{nI(U;X|F)\text{-}R_X}$ codeword sequences.

For each index tuple (w_f,w_u), randomly and independently generate $2^{nI(V;X|U,F)}$ sequences $v^n(w_f,w_u,w_v),w_v\in\{1,...,2^{nI(V;X|U,F)}\}$ according to $p(v^n)=\prod_{i=1}^{n}P_{V|UF}(v_i\,|\,u_i(w_f,w_u),f_i(w_f))$. Then distribute $v^n(w_f,w_u,w_v)$ uniformly at random into 2^{nR_C} Bins $r_v\in\{1,2,...,2^{nR_C}\}$, $r_v\in\{1,2,...,2^{nR_C}\}$. Each bin consists of $2^{nI(V;X|U,F)\text{-}R_C}$ codeword sequences.

Encoding. For a given source sequence x^n, the encoder would keep looking for the $f^n(w_f)$ which is jointly typical with x^n since the number is more than $2^{nI(X;F)}$. By the Covering Lemma in [18] Chapter 3.2, the eligible $f^n(w_f)$ would exist. Choose one that is jointly typical with (x^n, f^n) randomly and send the corresponding index w_f to the decoder.

Then the encoder would keep looking for a $u^n(w_f, w_u)$ which is jointly typical with (x^n, f^n) since the number is more than $2^{nI(U;X|F)}$. By the Covering Lemma, the eligible $u^n(w_f, w_u)$ would exist. Choose one index w_u that in the corresponding bin randomly and send it to the decoder.

Finally the encoder would keep looking for a $v^n(w_f, w_u, w_v)$ which is jointly typical with (x^n, f^n, u^n) since the number is more than $2^{nI(V;X|U,F)}$. By the Covering Lemmain, the eligible $v^n(w_f, w_u, w_v)$ would exist. Choose one index w_v that in the corresponding bin randomly and send it to the decoder.

Decoding. According to the system model, Bob observes B^n and receives Y^n from Alice. That is to say, Bob receives the indices $Y^n(\bar{w}_f, \bar{w}_u, \bar{w}_v)$ and side information B^n. At the view of Zve, Zve receives the indices $Z^n(\tilde{w}_f, \tilde{w}_u, \tilde{w}_v)$ and side information E^n. The decoder would keep looking for the unique u^n which is jointly typical with (b^n, f^n) in the bin $\mathcal{C}_1(r_u)$ since the number is less than $2^{nI(U;B|F)}$. By the Packing Lemma in [18] Chapter 3.7, it will find the correct u^n with high probability.

The decoder would keep looking for the unique v^n which is jointly typical with (b^n, f^n, u^n) in the bin $\mathcal{C}_2(r_v)$ since the number is less than $2^{nI(V;B|F,U)}$. By the Packing Lemma, it will find the correct v^n with high probability. Then we can calculate to get the s^n. According to the s^n and f^n, we can reconstruct source and get the estimated source $\hat{x}^n$.

Errors and constraints. Symbol 'ξ' denotes the event "An error occurred during the encoding or decoding steps", we consider its probability as follows:

Record the typical error of side information as event ξ_1 from properties of typical sequences, there exists a sequence $\lim_{n\to\infty}\eta_n = 0$ makes the inequality $P(\xi_1)=P\{(X^n,F^n,B^n,E^n) \notin \mathrm{T}_\varepsilon{}^n(X,F,B,E)\} \le \eta_n$ work. Similarly, record the typical error of channels as event ξ_2. Its error probability is $P(\xi_2)=P\{(F^n,Y^n,Z^n) \notin \mathrm{T}_\varepsilon{}^n(F,Y,Z)\} \le \eta_n$.

In the first step of encoding, it would find the sequence which is jointly typical with f^n. Record the error of finding no sequence as event ξ_3. There exists upper bound of error probability $\lim_{n\to\infty}\gamma_n \to 0$, then we have $P(\xi_3) \le \gamma_n$.

Record the errors in the second and third steps of encoding as event ξ_4 and event ξ_5, respectively. There also exists upper bound of error probability $\lim_{n\to\infty}\gamma_n \to 0$, then we have $P(\xi_4) \le \gamma_n$ and $P(\xi_5) \le \gamma_n$.

In the first step of decoding, it would find the sequence which is jointly typical with (B^n, f^n). Record the error of finding no sequence as event ξ_6. There exists upper bound of error probability $\lim_{n\to\infty}\gamma_n \to 0$, then we have $P(\xi_6) \le \gamma_n$.

Record the errors in the first and second steps of encoding as event ξ_7 and event ξ_8. There also exists upper bound of error probability $\lim_{n\to\infty}\gamma_n \to 0$, then we have $P(\xi_7)\le\gamma_n$ and $P(\xi_8)\le\gamma_n$.

Finally, the probability of event " An error occurred during the encoding or decoding steps" is

$$P(\xi)=2\eta_n+6\gamma_n\,. \tag{11}$$

4. Gaussian Noise Wiretap Channel based on the System Model

In this section, we consider the Gaussian noise wiretap channel based on the system model which is shown in Fig.3. Gaussian additive noise power of the legitimate channel is represented as $N_1\sim\mathcal{N}(0,P_y)$, side information is represented as $N_b\sim\mathcal{N}(0,P_b)$ and the gain of the channel component is represented as g_1. The power of the state information is represented as $N_s\sim\mathcal{N}(0,P_s)$. Gaussian additive noise power of the wiretap channel is represented a $N_2\sim\mathcal{N}(0,P_z)$, side information is represented as $N_e\sim\mathcal{N}(0,P_e)$ and the gain of the channel component is represented as g_2. Assume average power constraint P on F satisfies the inequality $\frac{1}{n}\sum_{i=1}^{n}E[F_i^2]\le P$.According to the encoding scheme in this paper, the sequence Bob received is

$$Y^n(\overline{w}_f,\overline{w}_u,\overline{w}_v)=g_1F^n(w_f,w_u,w_v)+N_1\quad , \tag{12}$$

The sequence Zve received is

$$Z^n(\tilde{w}_f,\tilde{w}_u,\tilde{w}_v)=g_2F^n(w_f,w_u,w_v)+N_2\,. \tag{13}$$

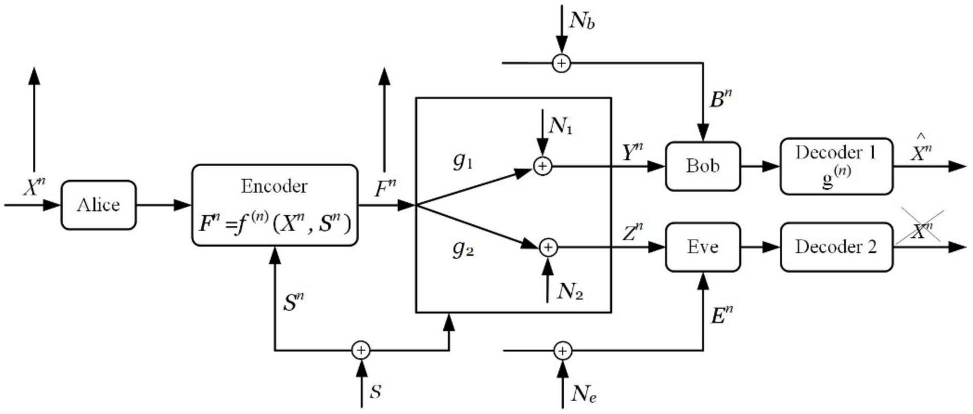


Figure. 3 Gaussian noise wiretap channel based on the system model.

Euclidean distance on $\mathbb{R}$ is used to measure distortion $d(x,\hat{x})=(x-\hat{x})^2$ at Bob over the Gaussian wiretap channel. We introduce equivocation rate [19] $\Delta\in\mathbb{R}$ to denotes the uncertainty of the information received by Eve. It can be expressed by the form $\frac{1}{n}H(X^n\,|\,Z^n,E^n)$=$\Delta+\delta$. Considering that $I_{\mathcal{DE}}=2^{2\Delta}/(2\pi e)$ denotes the minimum mean-square error of any estimator of source at Eve. Thus $\Delta=\frac{1}{2}\log_2(2\pi e)I_{\mathcal{DE}}$. It is worth mentioning that the information leakage $I_e\triangleq\frac{1}{n}I(X^n;Z^n,E^n)$

$$= H(X) - \frac{1}{n} H(X^n \mid Z^n, E^n) \leq H(X) - \Delta = \frac{1}{2}\log_2 \frac{1}{I_{\mathcal{DE}}}.$$

Definition 5. Tuple $(R,D,I_{\mathcal{DE}}) \in \mathbb{R}_+^3$ is said to be achievable if, for any $\delta > 0$ and $n \geq 1$, there exists an $n \geq 1$ code such that:

$$\mathrm{E}[\| X^n - g(B^n, Y^n) \|^2] \leq D + \delta, \tag{14}$$

$$\frac{1}{n} h(X^n \mid Z^n E^n) \leq \frac{1}{2}\log_2 I_{\mathcal{DE}} - \delta, \tag{15}$$

Theorem 2. Tuple $(R,D,I_{\mathcal{DE}}) \in \mathbb{R}_+^3$ is said to be achievable if

$$R \geq \frac{1}{2}\log_2 \frac{\det \Gamma_{FB} \cdot \mathrm{var}[V]}{\det \Gamma_{FV} \cdot \mathrm{var}[B]}, \tag{16}$$

$$D \geq \frac{\det\Gamma_{XBY} \cdot \det\Gamma_{\bar{V}XY}}{2\pi e \cdot \det\Gamma_{\bar{V}BY} \cdot \mathrm{var}[XY]}, \tag{17}$$

$$I_{\mathcal{D}\epsilon} \leq \frac{\det \Gamma_{\bar{F}X} \cdot \det \Gamma_{\bar{V}X} \cdot \det \Gamma_{B\tilde{F}} \cdot \det \Gamma_{EX}}{\det \Gamma_{\tilde{V}\tilde{F}} \cdot \det \Gamma_{BX} \cdot \det \Gamma_{E\tilde{F}}}, \tag{18}$$

Where $U = \emptyset$ and V denotes the auxiliary random variables on the finite set $\mathcal{V}$.

Proof. Analysis of the rate. From (5), we have $I(V;F|B)=h(F|B)\text{-}h(F|V) = \frac{1}{2}\log_2 \frac{\mathrm{var}[F \mid B]}{\mathrm{var}[F \mid V]}$. With $\mathrm{var}[F \mid B] = \frac{\det \Gamma_{FB}}{\mathrm{var}[B]}$, $\mathrm{var}[F \mid V] = \frac{\det \Gamma_{FV}}{\mathrm{var}[V]}$. Thus, $R \geq \frac{1}{2}\log_2 \frac{\det \Gamma_{FB} \cdot \mathrm{var}[V]}{\det \Gamma_{FV} \cdot \mathrm{var}[B]}$.

Analysis of the Distortion. From the Theorem 8.6.6 in [20], we have $\mathrm{E}(X - \hat{X}^2) \geq \frac{1}{2\pi \mathrm{e}} \cdot 2^{2\mathrm{h}(X)}$. Then we have $\mathrm{E}[d(X, \hat{X}(\bar{V}, B, Y))] \geq \frac{2^{2\mathrm{h}(X|\bar{V}BY)}}{2\pi \mathrm{e}}$. Thus, from (6), we have $D \geq \frac{2^{2\mathrm{h}(X|\bar{V}BY)}}{2\pi \mathrm{e}}$.

$$h(X \mid \bar{V}BY) = h(X \mid BY) + h(\bar{V} \mid XY) - h(\bar{V} \mid BY) = \frac{1}{2}\log_2 \frac{\mathrm{var}[X|BY]\,\mathrm{var}[\bar{V} \mid XY]}{\mathrm{var}[\bar{V} \mid BY]} = \frac{1}{2}\log_2 \frac{\det\Gamma_{XBY}\det\Gamma_{\bar{V}XY}}{\det\Gamma_{\bar{V}BY}\,\mathrm{var}[XY]}.$$

Thus, $D \geq \frac{\det\Gamma_{XBY} \cdot \det\Gamma_{\bar{V}XY}}{2\pi e \cdot \det\Gamma_{\bar{V}BY} \cdot \mathrm{var}[XY]}$.

Analysis of the minimum mean square error of the estimated source. From (7), we have

$$I_e \geq I(X;\tilde{V},\tilde{F},B) \text{-} I(X;B \mid \tilde{U},\tilde{F}) + I(X;E \mid \tilde{U},\tilde{F})$$
$$= I(X;\tilde{F}) + I(X;| \tilde{F}) + I(X;\tilde{V} \mid \tilde{F}) - I(X;B \mid \tilde{F}) + I(X;E \mid \tilde{F})$$
$$= [h(X) - h(\tilde{F} \mid X)] + [h(\tilde{F}) - h(X)] + [h(\tilde{V} \mid \tilde{F}) - h(\tilde{V} \mid X)] - [h(B \mid \tilde{F}) - h(B \mid X)] + [h(E \mid \tilde{F}) - h(E \mid X)]$$

Thus, $I_e = \frac{1}{2}\log_2 \frac{1}{I_{\mathcal{DE}}} \geq \frac{1}{2}\log_2 \frac{\mathrm{var}[\tilde{F}]\,\mathrm{var}[\tilde{V} \mid \tilde{F}]\,\mathrm{var}[B \mid X]\,\mathrm{var}[E \mid \tilde{F}]}{\mathrm{var}[\bar{F} \mid X]\,\mathrm{var}[\tilde{V} \mid X]\,\mathrm{var}[B \mid \tilde{F}]\,\mathrm{var}[E \mid X]}$. Finally,

$I_{\mathcal{D}\epsilon} \leq \frac{\det \Gamma_{\bar{F}X} \cdot \det \Gamma_{\bar{V}X} \cdot \det \Gamma_{B\tilde{F}} \cdot \det \Gamma_{EX}}{\det \Gamma_{\tilde{V}\tilde{F}} \cdot \det \Gamma_{BX} \cdot \det \Gamma_{E\tilde{F}}}$. This completes the proof.

Next, assuming that all channels of the Gaussian wiretap channel based on the system model are independent and identically distributed fading channels, and obey the Gaussian distribution with mean value of 0 and variance of 1. P_b and P_e denote side information noise power of legitimate channel and wiretap channel, respectively. P_y and P_z denote Gaussian additive noise power of legitimate channel and wiretap channel. P_z denotes the power of state information. Average power constraint by P . Choosing variables U , V and F as follows:

$$U = \emptyset , \tag{19}$$

$$V = X + S - \gamma N , \tag{20}$$

$$F = (\alpha X + \beta S - \gamma N)\sqrt{P} , \tag{21}$$

Where $\alpha \in (0,1)$, $\beta \in (0,1)$, $\gamma = \sqrt{1-\alpha^2-\beta^2}$, $N \sim \mathcal{N}(0,1)$, $X \sim \mathcal{N}(0,P)$. We have

$$F = [(\alpha-1)X + (\beta-1)S + V]\sqrt{P} , \tag{22}$$

$$\bar{V} = g_1(X + S - \gamma N) + N_1 , \tag{23}$$

$$\bar{F} = g_1[(\alpha-1)X + (\beta-1)S + V]\sqrt{P} + N_1 , \tag{24}$$

$$\tilde{V} = g_2(X + S - \gamma N) + N_2 , \tag{25}$$

$$\tilde{F} = g_2[(\alpha-1)X + (\beta-1)S + V]\sqrt{P} + N_2 . \tag{26}$$

Analysis of the rate.

Because $R \geq \frac{1}{2}\log_2 \frac{\mathrm{var}[F \mid B]}{\mathrm{var}[F \mid V]}$, $\mathrm{var}[F \mid B] = \frac{\det \Gamma_{FB}}{\mathrm{var}[B]}$, $\Gamma_{FB} = \begin{pmatrix} P(\alpha^2+\beta^2P_s+\gamma^2) & \alpha\sqrt{P} \\ \alpha\sqrt{P} & 1+P+P_b \end{pmatrix}$, we have

$$\mathrm{var}[F \mid B] = \frac{P[\alpha^2(P+P_b)+\beta^2P_s(1+P+P_b)+\gamma^2(1+P+P_b)]}{1+P+P_b} .$$

Similarly, because $\mathrm{var}[F \mid V] = \frac{\det \Gamma_{FV}}{\mathrm{var}[V]}$ and $\Gamma_{FV} = \begin{pmatrix} P(\alpha^2+\beta^2P_s+\gamma^2) & \sqrt{P}(\alpha+\beta+\gamma^2) \\ \sqrt{P}(\alpha+\beta P_s+\gamma^2) & 1+P_s+\gamma^2 \end{pmatrix}$, we have

$$\mathrm{var}[F \mid V] = \frac{P_sP[(\alpha-\beta)^2+\gamma^2(\beta-1)^2]+\gamma^2P(\alpha-1)^2}{1+P_s+\gamma^2} .$$

Analysis of the distortion. $D \geq \frac{\det\Gamma_{XBY} \cdot \det\Gamma_{\bar{V}XY}}{2\pi e \cdot \det\Gamma_{\bar{V}BY} \cdot \mathrm{var}[XY]}$. From (17), (18) and (19), we have

$$\Gamma_{XBY} = \begin{pmatrix} 1 & 1 & (\alpha-1)\sqrt{P} \\ 1 & 1+P+P_b & \alpha\sqrt{P} \\ (\alpha-1)\sqrt{P} & \alpha\sqrt{P} & P+P_y \end{pmatrix} .$$

From (19) and (20), we have $\Gamma_{\bar{V}XY} = \begin{pmatrix} 1+P_s+\gamma^2+P_y & 1 & (\alpha+\beta P_s+\gamma^2)\sqrt{P} \\ 1 & 1 & \alpha\sqrt{P} \\ (\alpha+\beta P_s+\gamma^2)\sqrt{P} & \alpha\sqrt{P} & P+P_y \end{pmatrix}$.

From (17) and (for20), we have $\Gamma_{\bar{V}BY}=\begin{pmatrix} 1+P_s+\gamma^2+P_y & 1 & (\alpha+\beta P_s+\gamma^2)\sqrt{P} \\ 1 & 1+P+P_b & \alpha\sqrt{P} \\ (\alpha+\beta P_s+\gamma^2)\sqrt{P} & \alpha\sqrt{P} & P+P_y \end{pmatrix}$.

Analysis of the minimum mean square error of the estimated source.

$I_{\mathcal{D}\epsilon}\le\dfrac{\det\Gamma_{\bar{F}X}\cdot\det\Gamma_{\bar{V}X}\cdot\det\Gamma_{B\tilde{F}}\cdot\det\Gamma_{EX}}{\det\Gamma_{\tilde{V}\tilde{F}}\cdot\det\Gamma_{BX}\cdot\det\Gamma_{E\tilde{F}}}$, $\Gamma_{\tilde{V}\tilde{F}}=\begin{pmatrix} 1+P_s+\gamma^2 & \sqrt{P}(\alpha+\beta P_s+\gamma^2) \\ \sqrt{P}(\alpha+\beta P_s+\gamma^2) & P(\alpha^2+\beta^2 P_s+\gamma^2)+P_z \end{pmatrix}$.

Similarly, the determinants of the remaining matrices in the inequality are obtained respectively, so that $I_{\mathcal{D}\epsilon}$ can be obtained.

Considering the different Gaussian additive noise, the side information is also different, we consider different situations to analyze the rate, distortion rate and leakage rate of the scheme proposed in this paper. When P_s is constant, there are four cases, as shown in Table.1. Then we discuss the situation of changing P_s.

Table 1 Cases where P_s *is constant*

	$P_b < P_e$	$P_b > P_e$
$P_y < P_z$	eg. Case1	eg. Case2
$P_y > P_z$	eg. Case3	eg. Case4

Simplify formulas that contain α, β and γ by $\gamma^2=1-\alpha^2-\beta^2$. We have R, D and $I_{\mathcal{D}\epsilon}$ with α and β. Then we select the appropriate specific value to R, D and $I_{\mathcal{D}\epsilon}$. The unit of R, D and $I_{\mathcal{D}\epsilon}$ bits/source-bit is omitted below. Considering the optimal trade-off among rate, distortion and minimum mean square error of source estimation, finding the optimal trade-off point is transformed into the optimization problem of maximizing the target value. Let '*weight*' be the target. *weight* is shown below. Function atan() is the arctangent function.

$$weight=\text{atan}(R)+1/\text{atan}(D)+\text{atan}(I_{\mathcal{D}\mathcal{E}}) \tag{27}$$

Case1. $P_y=0.5, P_z=1$, $P_b=0.5, P_e=1$, $P=1$, $P_s=1$.

Case2. $P_y=0.5, P_z=1$, $P_b=1, P_e=0.5$, $P=1$, $P_s=1$.

Case3. $P_y=1, P_z=0.5$, $P_b=0.5, P_e=1$, $P=1$, $P_s=1$.

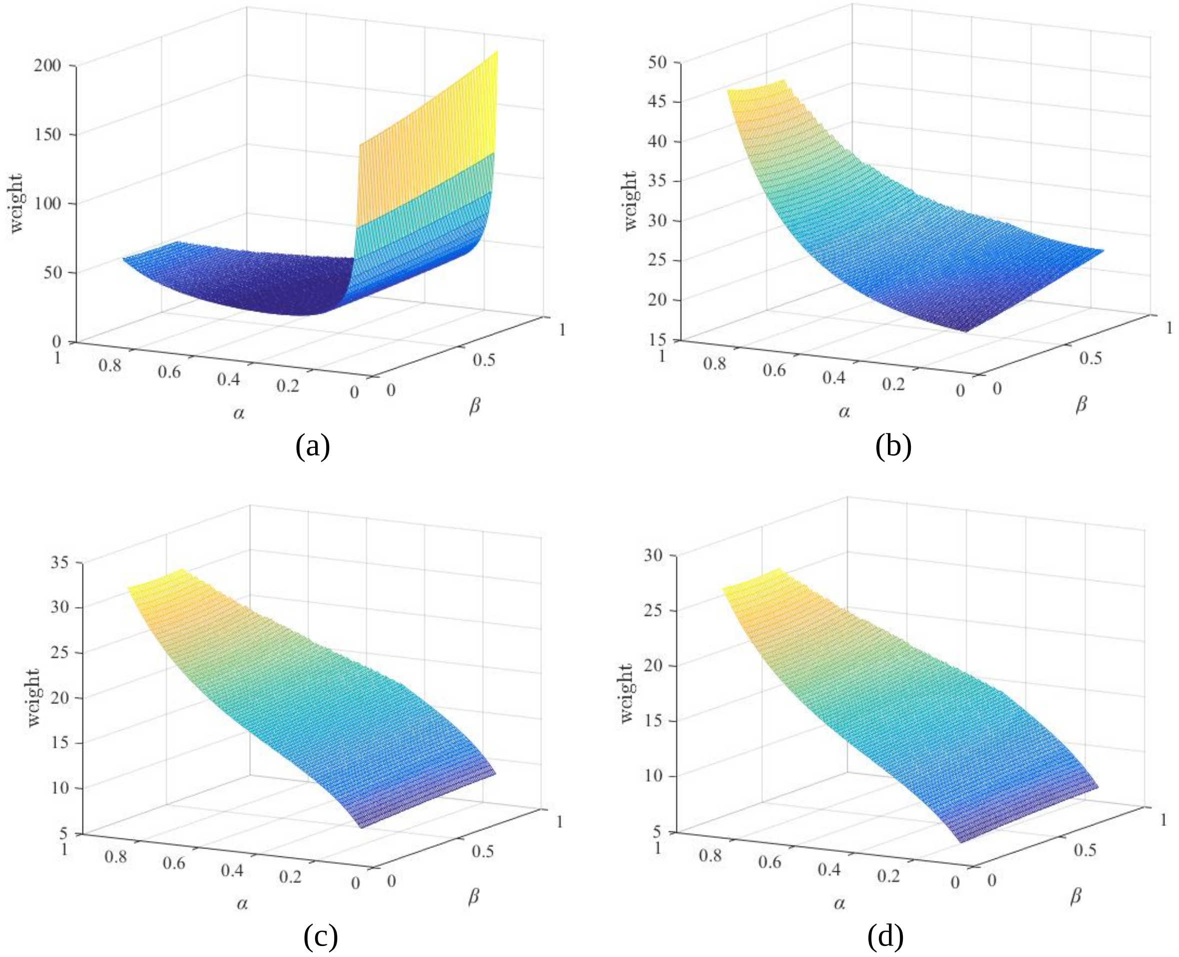
Case4. $P_y=1, P_z=0.5$, $P_b=1, P_e=0.5$, $P=1$, $P_s=1$.

Fig.4 (a) depicts the graph of the target values with respect to α and β in case 1. The maximum target value is 194.0052 when $\alpha=0.1$, $\beta=0.9$, $\gamma=0.42$. Meanwhile, $R=0.7315$, $D=0.0052$, $I_{\mathcal{D}\epsilon}=0.8368$.

Fig.4 (b) depicts the graph of the target values with respect to α and β in case 2. The maximum target value is 46.2279 when $\alpha=0.1$, $\beta=0.9$, $\gamma=0.42$. Meanwhile, $R=0.5704$, $D=0.0220$, $I_{\mathcal{D}\epsilon}=0.2571$.

Fig.4 (c) depicts the graph of the target values with respect to α and β in case 3. The maximum target value is 31.9783 when $\alpha=0.9$, $\beta=0.43$, $\gamma=0.071$. Meanwhile, $R=0.3031$, $D=0.0332$, $I_{\mathcal{D}\epsilon}=0.4053$.

Fig.4 (d) depicts the graph of the target values with respect to α and β in case 4. The maximum target value is 26.8701 when $\alpha = 0.9$, $\beta = 0.43$, $\gamma = 0.071$. Meanwhile, $R = 0.3585$, $D = 0.0400$, $I_{\mathcal{D}\epsilon} = 0.2812$.



(a)

(b)

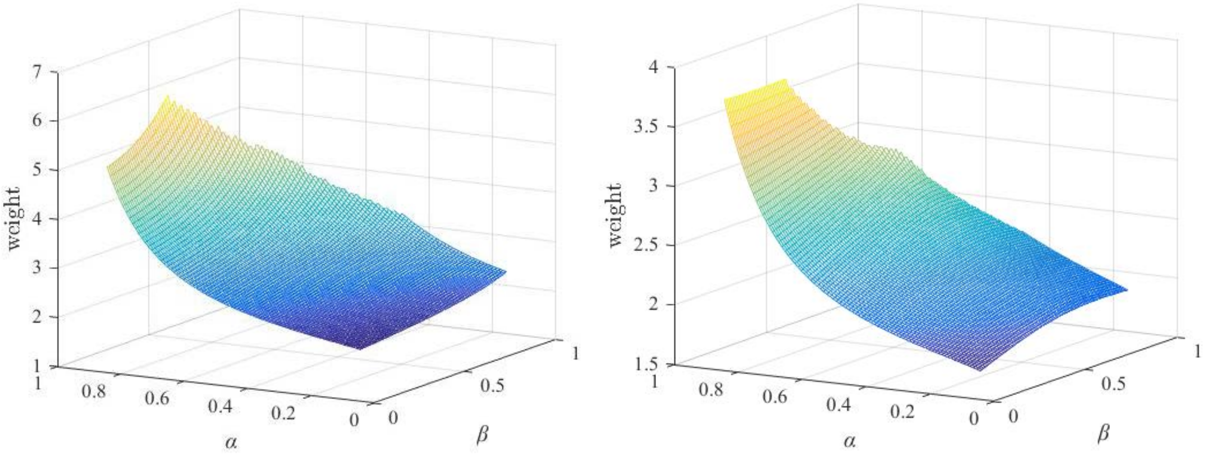
(c)

(d)

Figure. 4 The target values with respect to α and β in 4 cases

Finally, we consider the situation of changing P_s. Fig.5 (a) depicts the graph of the target values with respect to α and β when we decrease the value of P_s to 0.5 in case 1. The maximum target value is 6.0487 which also decreases when $\alpha = 0.9$, $\beta = 0.43$, $\gamma = 0.071$. Meanwhile, $R = 0.4899$, $D = 0.0158$, $I_{\mathcal{D}\epsilon} = 0.2005$.

Fig.5 (b) depicts the graph of the target values with respect to α and β when we increase the value of P_s to 1.5 in case 1. The maximum target value is 3.7056 which decreases conversely when $\alpha = 0.9$, $\beta = 0.1$, $\gamma = 0.42$. Meanwhile, $R = 0.3413$, $D = 0.0178$, $I_{\mathcal{D}\epsilon} = 0.3045$.



(a) (b)

Figure. 5 Cases where the power of state informationin changes

Based on the above experimental results, it is concluded as follows. In case 1, the target value reaches the maximum value of four cases. Meanwhile, the information leakage rate $I_e = 0.1286$. Distortion also reaches the minimum value in several cases. It is clear that case 1 is optimal. In addition, the results obtained are higher than those in the secure lossy source transmission scheme proposed in [12] and the value of quantitative $I_{\mathcal{D}\epsilon}$ is higher than that of the optimal scheme proposed in [19]. Rate and distortion are used to measure its reliability and quantitative $I_{\mathcal{D}\epsilon}$ is used to measure its security. The comparison shows that the transmission model and its coding scheme proposed in this paper have certain security and reliability.

However, the situation in case 1 can not be maintained at any time in practice, so other possible actual situations should be considered. Considering case 2, the results show that rate and quantitative $I_{\mathcal{D}\epsilon}$ both decrease while the distortion rate increases. The target values of case 3 and case 4 relatively decrease and the target value of case 4 is the smallest. Thus, case 4 has the worst situation. Through the analysis, it can be concluded that the influence of the noise power of the side information on rate constrained domain is smaller than that of Gaussian additive noise. Moreover, when the state information is changed under the optimal condition, all elements decrease. Thus, tough we have foud some rules, the optimal powers of side information and state information should be found to meet the maximum $I_{\mathcal{D}\epsilon}$, that is to say, to meet the minimum information leakage rate.

5. Conclusions

In this paper, we construct a secure lossy transmission model with side information and state information over wiretap channel. According to the system model proposed in this paper, we design a random coding scheme based on double binning technology. Then we derive the inner bound of rate, distortion and information leakage rate. Afterwards, the Gaussian noise wiretap channel based on the system model is analyzed. The simulation results show that the trade-off between rate, distortion and information leakage rate is optimal when Gaussian additive noise power of legitimate channel is lower than that of wiretap channel and the side information noise of legal receiver is smaller than that of eavesdropper. In this situation, the rate reaches 0.7315 bits / source bit, the distortion reaches 0.0052 bits / source bit and the information leakage rate reaches 0.1286 bits / source bit.

Compared with the data in other references, it is proved that the model and its random coding scheme are reliable and secure.

References

[1] B. Biggio, g. fumera, P. Russu, L. Didaci and F. Roli, "Adversarial Biometric Recognition : A review on biometric system security from the adversarial machine-learning perspective," in IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 31-41, Sept. 2015.

[2] C. Zhou, "Comments on “Light-Weight and Robust Security-Aware D2D-Assist Data Transmission Protocol for Mobile-Health Systems”," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, pp. 1869-1870, July 2018.

[3] K. Li, W. Zhang, C. Yang and N. Yu, "Security Analysis on One-to-Many Order Preserving Encryption-Based Cloud Data Search," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 9, pp. 1918-1926, Sept. 2015.

[4] S. Sultana, M. Shehab and E. Bertino, "Secure Provenance Transmission for Streaming Data," in IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 8, pp. 1890-1903, Aug. 2013.

[5] R. Al-Jaljouli, J. Abawajy, M. M. Hassan and A. Alelaiwi, "Secure Multi-Attribute One-to-Many Bilateral Negotiation Framework for E-Commerce," in IEEE Transactions on Services Computing, vol. 11, no. 2, pp. 415-429, 1 March-April 2018.

[6] C. E. Shannon, "Communication theory of secrecy systems," in The Bell System Technical Journal, vol. 28, no. 4, pp. 656-715, Oct. 1949.

[7] A. D. Wyner, "The wire-tap channel," in The Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[8] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," in IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 339-348, May 1978.

[9] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," in IEEE Transactions on Information Theory, vol. 19, no. 4, pp. 471-480, July 1973.

[10] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," in IEEE Transactions on Information Theory, vol. 22, no. 1, pp. 1-10, January 1976.

[11] Y. Chia and H. Chong, "On Lossy Source Coding With Side Information Under the Erasure Distortion Measure," in IEEE Transactions on Information Theory, vol. 61, no. 12, pp. 6475-6484, Dec. 2015.

[12] J. Villard and P. Piantanida, "Secure lossy source coding with side information at the decoders," 2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Allerton, IL, pp. 733-739, 2010.

[13] J. Villard and P. Piantanida, "Secure Multiterminal Source Coding With Side Information at the Eavesdropper," in IEEE Transactions on Information Theory, vol. 59, no. 6, pp. 3668-3692, June 2013.

[14] Y. Xu, X. Guang and J. Lu, "Vector Gaussian Successive Refinement With Degraded Side Information," 2019 IEEE International Symposium on Information Theory (ISIT), Paris, France, 2019, pp. 1832-1836.

[15] O. O. Koyluoglu, R. Soundararajan and S. Vishwanath, "State amplification under masking constraints," 2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, pp. 936-943,2011.

[16] T. S. Han and M. Sasaki, "Wiretap Channels With Causal State Information: Strong Secrecy," in IEEE Transactions on Information Theory, vol. 65, no. 10, pp. 6750-6765, Oct. 2019.

[17] A. E. Gamal and Y. H. Kim, Network Information Theory. Cambridge University Press, 2011.

[18] O. Günlü, K. Kittichokechai, R. F. Schaefer and G. Caire, "Controllable Identifier Measurements for Private Authentication With Secret Keys," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 1945-1959, Aug. 2018.

[19] J. Villard, P. Piantanida and S. Shamai, "Secure Transmission of Sources Over Noisy Channels With Side Information at the Receivers," in IEEE Transactions on Information Theory, vol. 60, no. 1, pp. 713-739, Jan. 2014.

[20] T. Cover and J. Thomas, Elements of Information Theory. A John Wiley & Sons,inc.,Publiction,2006.